

# HomeUse Installation Guide For Symantec Endpoint Protection (SEP) 11 Windows 2000/2003/XP/Vista/7

Information and Protection

October 2009

## Table of Content

1	INTRODUCTION.....	2
2	AntiVirus Software Home Use License Policy .....	2
2.1	Authorized Users: .....	2
2.2	Department of State Restrictions: .....	2
2.3	Usage Stipulations: .....	2
2.4	Installation Support: .....	3
3	Pre-Installation Notes.....	3
4	System Requirements.....	4
5	Installation of Symantec Endpoint Protection (SEP) .....	5
6	SEP Firewall Configuration.....	11

# 1 INTRODUCTION

As part of the Corporate License Agreement negotiated with Symantec, on behalf of the Department of State (DoS), Symantec Endpoint Protection (SEP) software is authorized to be disseminated to DoS employees and contractors for residential use under the Home Use License Agreement as negotiated under the terms and conditions of License ID# 12457802.

Questions concerning the Corporate License Agreement with the Symantec Corporation should be directed to the AntiVirus Program Manager at (202) 203-5172.

## 2 AntiVirus Software Home Use License Policy

The Department of State policy concerning the removal and installation of Symantec Endpoint Protection (SEP) software products is as follows: The Department has entered into a license agreement to utilize Symantec Endpoint Protection (SEP) software. The software is not free. Giving copies to friends and relatives is NOT AUTHORIZED, is a violation of the license agreement, and may subject the employee to prosecution. Duplication of the licensed AntiVirus software is authorized for the AntiVirus Office ONLY.

### 2.1 Authorized Users:

1. All Department of State employees.
2. All other U.S. Federal Government Employees and Contractors to the extent they are engaged in the performance of work for the Department of State or utilizing the Department of State systems.
3. Home office, personal computer use for the end-user identified above in accordance with the Symantec Home Use License Addendum, as modified by the mutual agreement of the parties.

### 2.2 Department of State Restrictions:

1. US Citizen direct hire supervisor must approve in advance each installation of SEP software as official business.
2. Per STATE 100359, Post is authorized to distribute HomeUse CDs to Locally Engaged Staff (LES) as long as they have complied with paragraph 5 (determining host country's import laws) and 7 (reply via telegram to IRM\OPS\ITI\SI\AV). If Post has any further questions concerning the distribution of CDs to LESs, please send an email (questions only) to [virus2@state.gov](mailto:virus2@state.gov) and a reply will be sent soonest.
3. The software is provided "AS IS" and without technical support from Symantec or the Department of State. Employees will use the software at their own risk.

### 2.3 Usage Stipulations:

Department of State employees and contractors who install AntiVirus software on their privately owned PC's must adhere to the following stipulations:

1. The media (e.g. diskettes) used to install the AntiVirus software may not subsequently be used on a United States Government (USG) system.
2. The media (e.g. diskettes) used to transfer information from a privately owned PC to a USG system must be checked for viruses on a standalone system immediately before the transfer.
3. Only unclassified, non-sensitive USG information may be processed on privately owned PC's. Department of State policy strictly prohibits the processing of classified national security information (i.e. Confidential, Secret and Top Secret) and Sensitive but Unclassified (SBU) information on privately owned PC's.
4. The media (e.g. diskettes) introduced into classified Automated Information Systems (AIS) immediately becomes classified because of potential data migration and must be marked and protected as such. Consequently, media used on a classified computer either to upload or download information cannot subsequently be used on an unclassified system.

## **2.4 Installation Support:**

Bureau and Post Systems Managers are neither required, nor tasked with the responsibility of installing or maintaining AntiVirus software at the employee's residence. Installation of the AntiVirus products and the maintenance of periodic "Definition Update Files" fall solely on the employee. In addition, employees and contractors removing and installing the AntiVirus software on their home computers will do so at their own risk. Questions concerning the above approval of the use of AntiVirus software on privately owned PC's should be directed to the Systems Integrity Division Virus Incident Response Team (IRM/OPS/ITI/SI) at (202) 203-5172.

## **3 Pre-Installation Notes**

- SEP protects endpoint computing devices (personal computers) from virus threats, and risks, and provides three layers of protection, network threat protection, proactive threat protection and antivirus and antispyware protection.
- For network protection SEP contains a personal Firewall and Intrusion Protection features, misconfiguration of these features can have an adverse impact on the ability to connect to the internet. The creation of additional rules within the Firewall and IPS features may increase security but could also impact Internet access. Disabling these features may be necessary.
- Proactive Threat Protection includes behavior-based security that identifies online threats such as worms, viruses, Trojan horses, and keystroke loggers by their actions and characteristics, not with traditional security signatures. Proactive Threat Protection analyzes the threat's behavior against hundreds of detection modules to determine whether the active processes are safe or malicious.
- Antivirus and Antispyware Threat Protection prevents infections on computers by scanning the boot sector, memory, and files for viruses, spyware, and security risks. Antivirus and antispyware threat protection uses the virus and the security risk signatures that are found in virus definitions files. This protection also protects computers by blocking security risks before they install if this action would not leave the computer in an unstable state.

## 4 System Requirements

### **For computers utilizing SEP Client 32 bit Software:**

- Processor – 400 MHz Intel Pentium III (1 GHz for Windows Vista)
- Operating Systems - A The following operating systems are supported:
  - Windows® 2000 Professional/Server/Advanced Server with SP3 or later
  - Windows XP Home Edition/Professional/Tablet PC Editions
  - Windows Server 2003 Web/Standard/Enterprise/Datacenter Editions
  - Windows Vista (x86)
- Memory 256 MB of Ram
- Hard Disk 600 MB
- Display – Super VGA (1,024x768) or higher-resolution video adapter and monitor
- Other requirements:
  - Internet Explorer 6.0 or later
  - Terminal Server clients connecting to a computer with antivirus protection have the following additional requirements:
    - Microsoft Terminal Server RDP (Remote Desktop Protocol) client
    - Citrix® Metaframe® (ICA) client 1.8 or later if using Citrix Metaframe server on Terminal Server

### **For computers utilizing SEP Client 64 bit Software:**

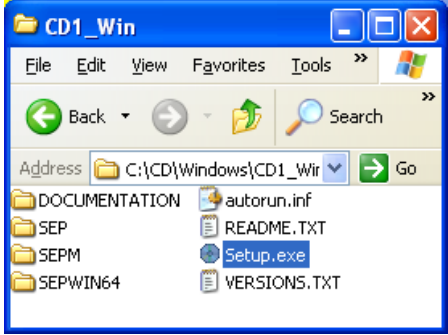
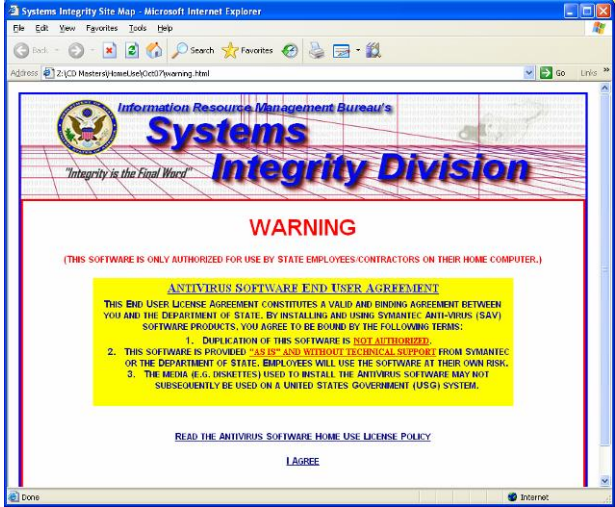
- Processor – 1 GHz on x64 only with the following processors:
  - Intel Xeon with Intel EM64T support
  - Intel Pentium IV with EM64T support
  - AMD 64-bit Opteron™
  - AMD 64-bit Athlon™
    - Note: Itanium is not supported.
- A Operating Systems - The following operating systems are supported:
  - Windows XP Professional x64 Edition with Service Pack 1 or later
  - Windows Server 2003 x64 Edition
  - Windows Vista (x64)
- Memory 256 MB of Ram
- Hard Disk - 700 MB
- Display – Super VGA ((1,024x768) or higher-resolution video adapter and monitor
- Other requirements:
  - Internet Explorer 6.0 or later

## 5 Installation of Symantec Endpoint Protection (SEP)

Installation of SEP will require the computer to be rebooted, perhaps more than once. Be prepared to reboot the computer when requested.

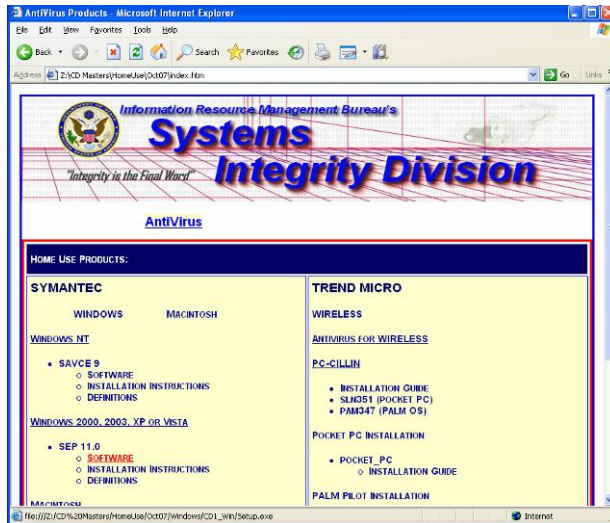
The screen shots shown below are typical for a computer running Windows XP. The dialog boxes you receive may differ.

**Table 5-1, SEP Installation**

Step	Action
1.	Uninstall all existing AntiVirus Software and reboot the computer.
2.	<p>If not using the web interface locate <b>Setup.exe</b> located in the <b>&lt;CD&gt;:\Windows\CD1_Win</b> folder on the CD and run <b>Setup.exe</b>.</p>  <p>Note: When Setup.exe is run in this manner the web pages will not be displayed.</p>
3.	<p>If not in the web interface skip this step. When “<b>WARNING</b>” page is displayed click on “<b>READ THE ANTIVIRUS SOFTWARE HOME USE LICENSE POLICY</b>” to review the policy or click on “<b>I AGREE</b>” to begin installation.</p> 

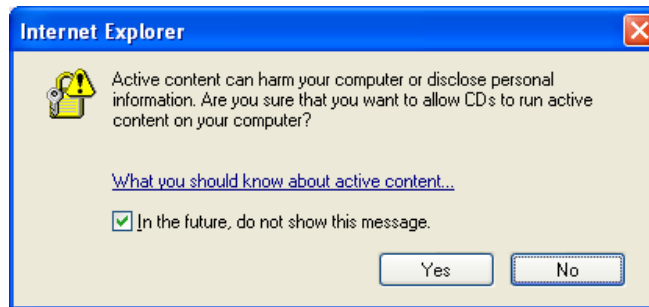
4.

If not in the web interface skip this step, otherwise locate “**Windows 2000, 2003, XP or VISTA**” on the left side of the page and click on the “**SOFTWARE**” under “**SEP 11.0**” (Shown in red in the screen capture below.)



5.

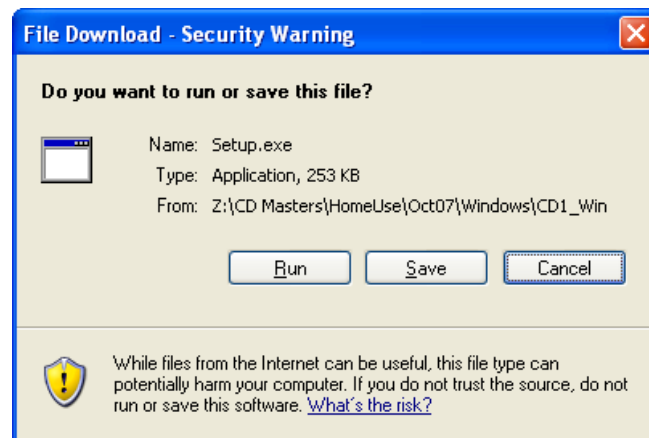
If not in the web interface skip this step, otherwise click **Yes**.



Note: Clicking **No** will discontinue the setup process.

6.

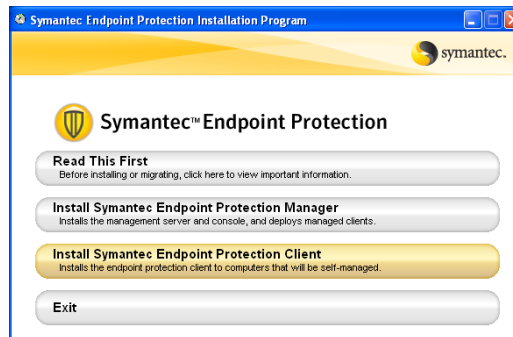
If not in the web interface skip this step, otherwise click **Run**.



7. You may get a security warning similar to the one below more than once. If so just click on **Run**.

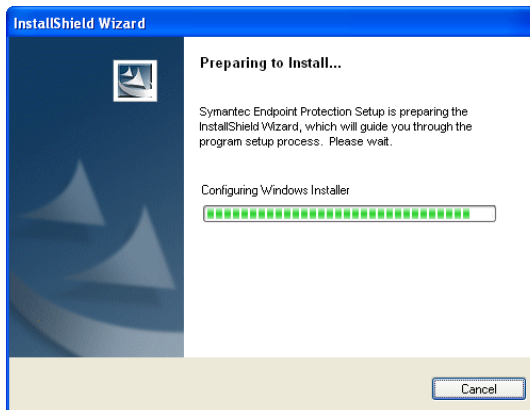


8. Once Setup.exe is running click on **Install Symantec Endpoint Protection Client**.



Note: **Install Symantec Endpoint Protection Manager** is disabled and not included on this CD.

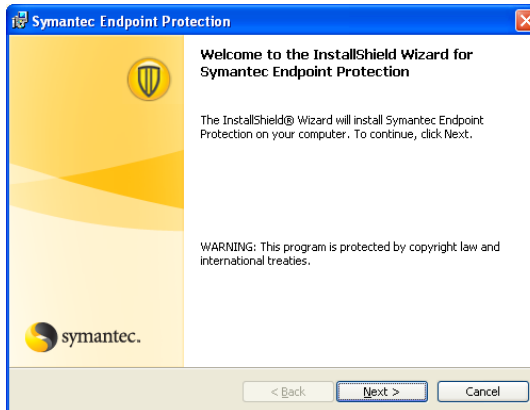
9. The InstallShield Wizard Opens.





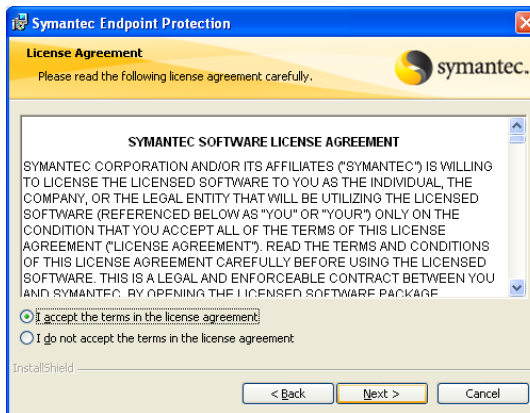
10.

In the **InstallShield Wizard for Symantec Endpoint Protection** dialog click **Next>**.



11.

Select **I accept the terms in the license agreement** then click **Next>**.

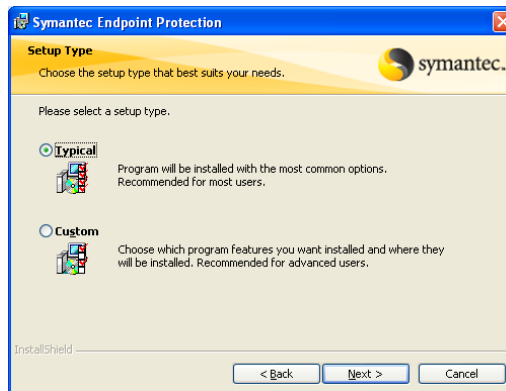


12.

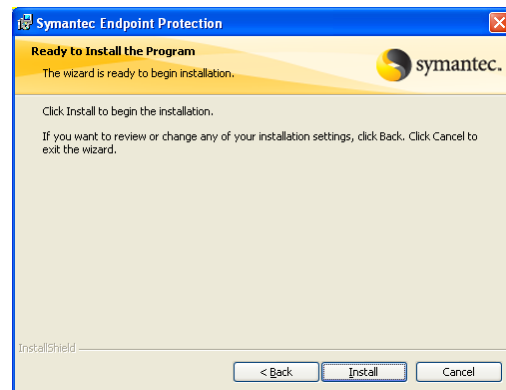
Select **Unmanaged Client** then click **Next>**.



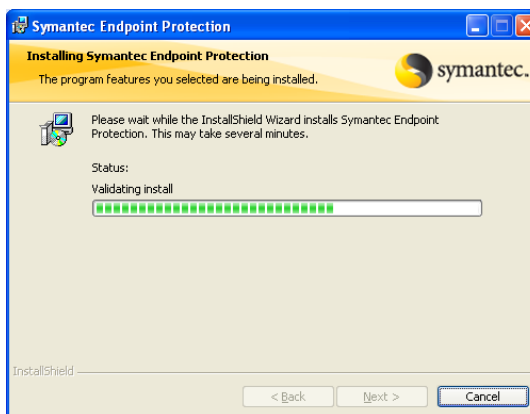
13. Select **Typical** and then click on **Next>**.

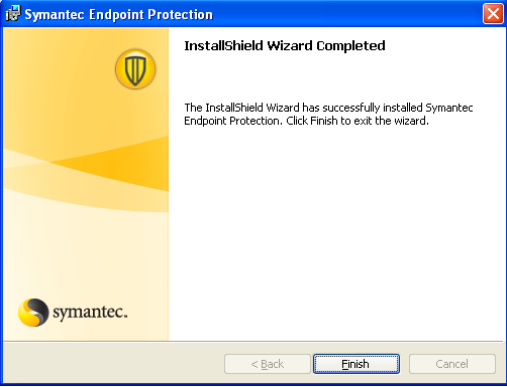

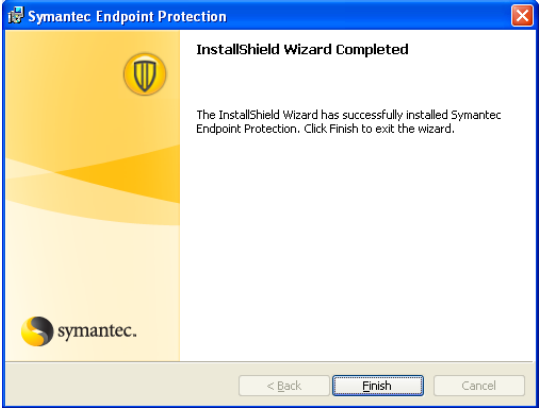


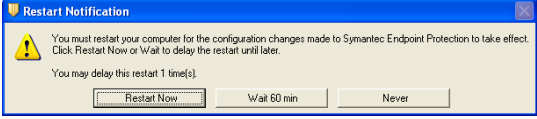
14. Click **Install**.



15. Installation continues. This process will take several minutes.



16.	<p>The <b>InstallShield Wizard Completed</b> dialog box is displayed. No action is required.</p> 
17.	<p>LiveUpdate will begin to run automatically. This process requires connection to the Internet and may take several minutes to complete. No action is required.</p> 
18.	<p>When LiveUpdate is completed the <b>InstallShield Wizard Completed</b> dialog box should still be displayed. Click <b>Finish</b>.</p> 

19.	<p>Reboot the computer by clicking on <b>Restart Now</b>.</p>  <p>Installation is complete.</p>
-----	---

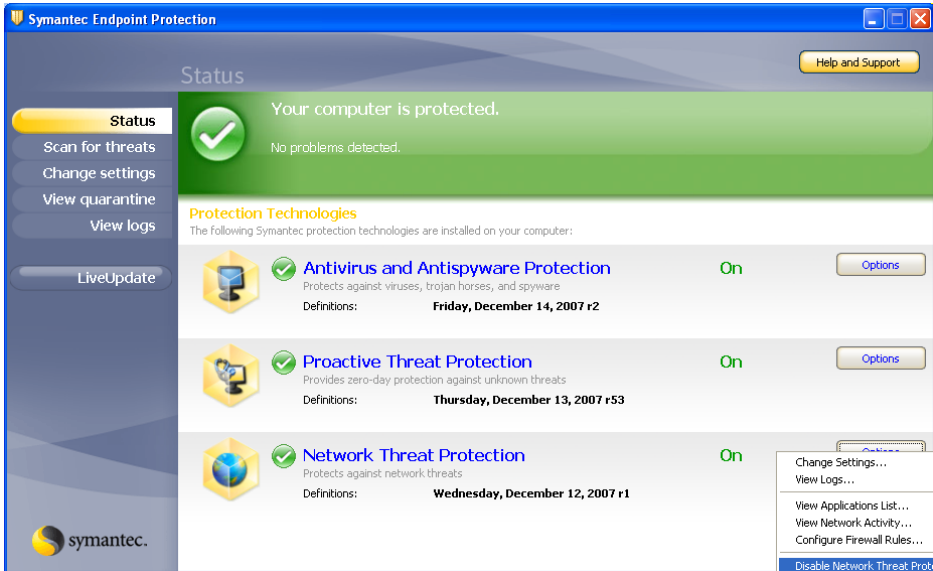
## 6 SEP Firewall Configuration

By default the SEP Firewall will allow all network traffic. If you wish to restrict network traffic you must reconfigure the firewall.

**Caution: Run only one firewall at a time. If the Operating System Firewall has a firewall you must disable one of the firewalls. Be sure you understand the impact of changes to the firewall. Even small changes may affect desired functions.**

The screen shots shown are typical Windows XP. The dialog boxes you receive may differ.

**Table 6-1, SEP Firewall Configuration**

Step	Action
1.	<p>To turn off the firewall in SEP open SEP by double clicking on the icon in the system tray or under the start menu click on <b>Start\Programs\Symantec Endpoint Protection\ Symantec Endpoint Protection</b>.</p> <p>In the lower right of the user interface click on the <b>Options</b> button next to <b>Network Threat Protection</b> and select <b>Disable Network Threat Protection</b>.</p>  <p>Note: If <b>Network Threat Protection</b> under <b>Proactive Threat Protection</b>, close the window then re-open <b>SEP (Symantec Endpoint Protection)</b>.</p>

2.

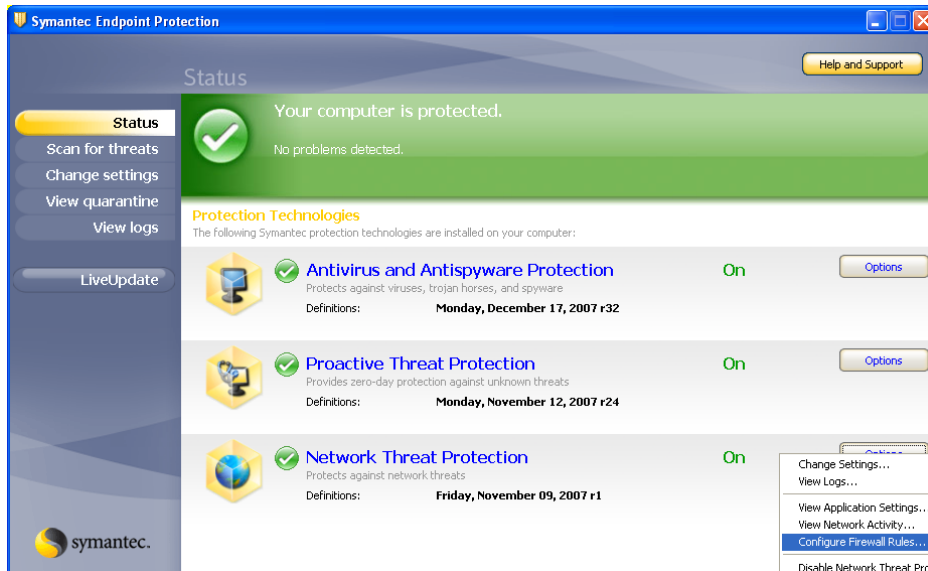
After a few minutes the firewall will be set to **Off**.



To turn the firewall on again click **Fix** in the red bar.

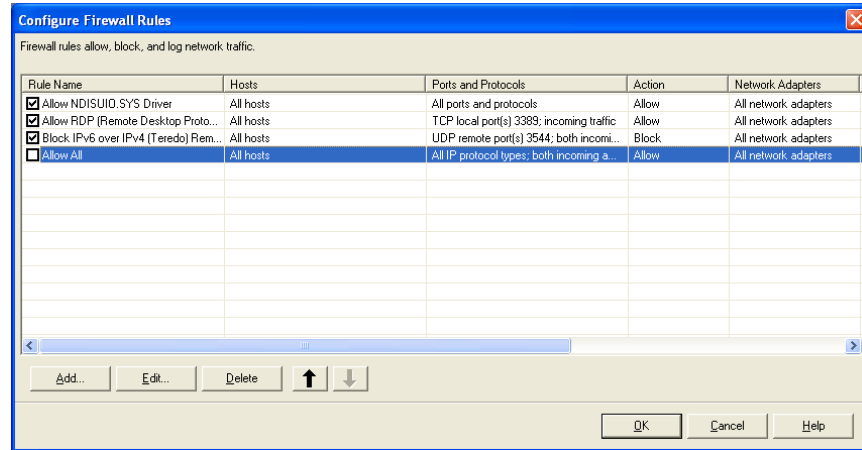
3.

To configure the firewall rules click on **Options** next to Network threat Protection and select **Configure firewall Rules...**



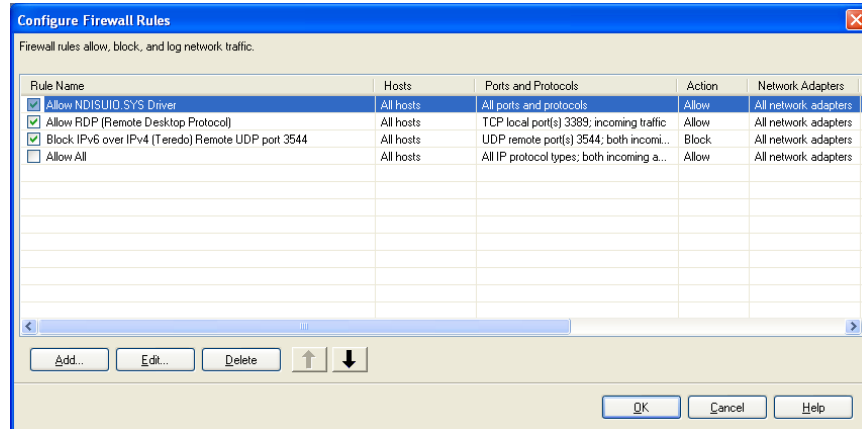
4.

To configure the firewall rules to block network traffic remove the check next to **Allow All**. Note: this may block desired network traffic and additional rules may need to be added to allow specific network traffic.

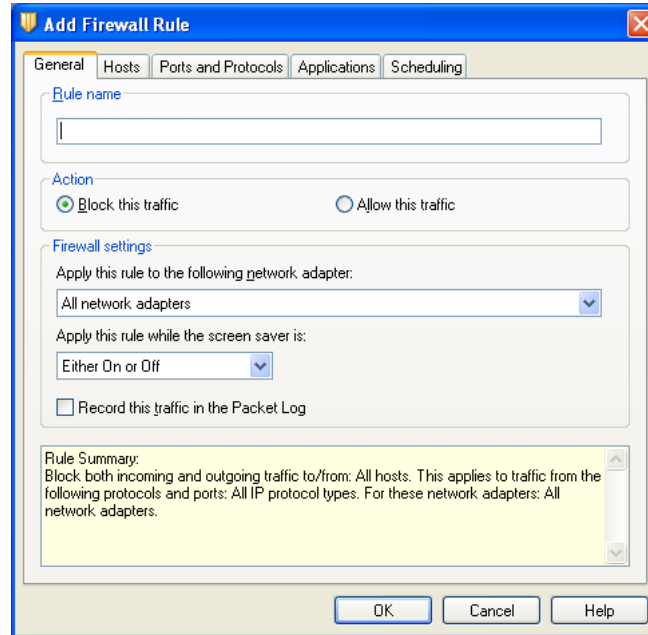


5.

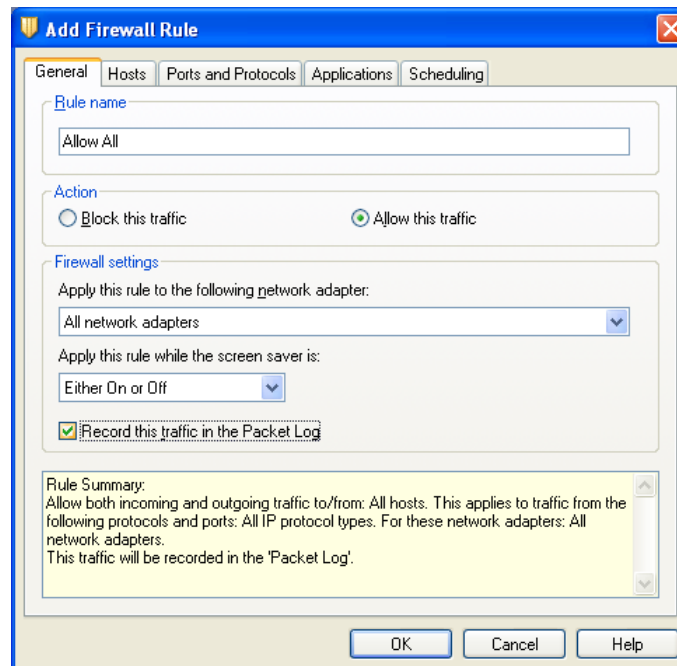
If **Allow All** is not listed, click **Add**.



6. Select the **General** tab at the top of the window.

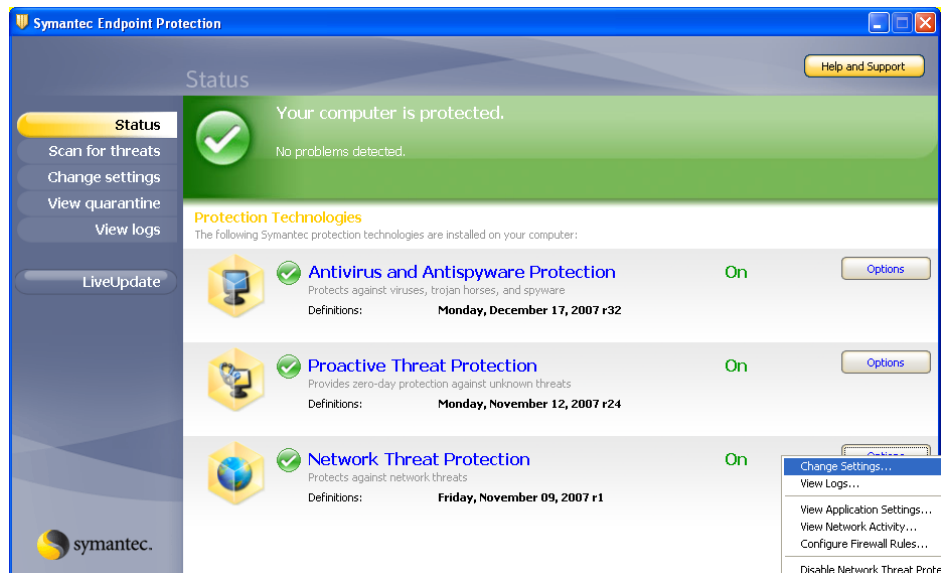


7. In the **Rule Name** section, type “**Allow All.**” Then select **Allow this traffic** in the **Action** section.

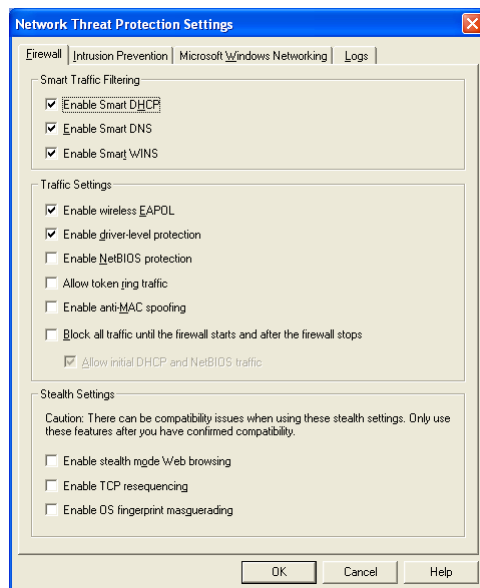




8. To configure the firewall setting click on **Options** next to Network threat Protection and select Change Settings.



9. To allow a specific traffic place a check next to the setting.  
To block a specific type of traffic remove the check next to the setting.  
For example: If you do not use wireless networking remove the check next to **Enable wireless EAPOL**.



10.	<p><b>Sample Firewall Configurations: To Enable network file and printer browsing</b></p> <ol style="list-style-type: none"> <li>1. Open the Symantec Endpoint Protection client interface.</li> <li>2. Click the "<b>Options</b>" button beside "<b>Network Threat Protection</b>". This will open a menu.</li> <li>3. Click "<b>Change Settings...</b>" in the menu. This will open the "<b>Network Threat Protection Settings</b>" page.</li> <li>4. Click the "<b>Microsoft Windows Networking</b>" tab.</li> <li>5. In the "<b>Setting</b>" section, put a check in the box beside "<b>Browse files and printers on the network</b>".</li> </ol> <p>If the server sharing the folders is also an unmanaged SEP 11 client, please follow the steps below on that client:</p> <p><b>To Enable network file and printer sharing</b></p> <ol style="list-style-type: none"> <li>1. Open the Symantec Endpoint Protection client interface.</li> <li>2. Click the "<b>Options</b>" button beside "<b>Network Threat Protection</b>". This will open a menu.</li> <li>3. Click "<b>Change Settings...</b>" in the menu. This will open the "<b>Network Threat Protection Settings</b>" page.</li> <li>4. Click the "<b>Microsoft Windows Networking</b>" tab.</li> <li>5. In the "<b>Setting</b>" section, put a check in the box beside "<b>Share my files and printers with others on the network</b>".</li> </ol>
-----	---

Please note that firewall settings can be complicated and it is not possible to include all possible configurations in this document. The examples above give the user an idea of how to configure the firewall but are not intended to be a complete reference on the subject of firewall configuration.